

AF INPUT of RQMS

Master Copy
CSS File:
IC Computer
Security Policy Paper

MEMORANDUM FOR THE CHAIRMAN,
COMPUTER SECURITY SUBCOMMITTEE

Subject: Computer Security Plan

1. Introduction and Background.

a. Introduction:

(1) This paper presents a plan which is oriented toward providing the intelligence community a means by which they can process Sensitive Compartmented Information in a safe, yet responsive, manner. The objective is to protect Sensitive Compartmented Information to the degree appropriate for its type and location, and at the lowest practical cost. Since security considerations can, and seriously do, affect the economical and effective use of ADP resources, it makes sense for the Computer Security Subcommittee to be intimately involved in the establishment and management of ADP security policy.

b. Background:

(1) The Intelligence Community does have a computer security problem. This problem has many interdependent aspects, but the most important ones stem from increasing operational requirements for secure and economical multi-level processing and the security deficiencies of contemporary automatic data processing systems (ADPS). Many other factors complicate this problem, however, and will be identified later.

(2) There are two key questions which must be answered if a long-term solution is to be forthcoming. The first question is "What can and must we do with contemporary ADPS to satisfy DCID 1/16?" Secondly, "What must we do to resolve security problems for future intelligence community ADPS?" The approach described here specifies that an investigation of present and future requirements/solutions must be included in an overall ADP security plan. Neither R&D nor interim solutions by themselves will do. We need both!!

2. The Plan: The paragraphs which follow describe the purpose, scope, and method of the ADP Security Plan. The problems which it is designed to resolve (or alleviate) and the assumptions upon which it is based are also noted. The critical tasks to be done are identified and their relative order of importance is indicated.

a. Purpose:

(1) Primary: To identify what must be done to provide for a long-term, comprehensive, and continuing solution to the more critical ADP security problems which face the Intelligence Community.

(2) Secondary: To provide the basis for a rapid and comprehensive response to DCID 1/16.

b. Scope: This plan covers all Intelligence Community ADP installations, equipment, and systems.

c. Method: A typical program/project planning approach is used for this plan. In implementing the plan, however, an USIB directive must be developed which establishes an Office of Primary Responsibility (OPR) for ADP security, with full responsibility, authority and resources. The plan itself directs certain actions to be performed, establishes milestones, and prescribes procedures for general implementation. The plan contains a number of activities which should be of a continuous and ongoing nature, and others which need to be done only once.

d. Problems: There are a number of problems in the ADP security field. The more immediate and important ones are:

(1) No single USIB organization at present has overall responsibility for all aspects of ADP security, including the development of ADP security policy, regulations, and procedures. Accompanying this situation is the fact that an overall ADP security "program" does not exist within the Intelligence Community.

(2) ADP security crosses a number of organizational, functional, and responsibility boundaries.

(3) The specific responsibilities of USIB elements (i.e., CIA, NSA, DIA) for ADP security, including their levels of involvement, are not clearly defined by existing regulations.

(4) As a reflection of the above, and especially with regard to problem 1, no single organization has all of the necessary resources to effectively accomplish all of the tasks required.

(5) Operational and/or quantitative definitions of "adequate protection" for any level of classification or type do not exist.

(6) There is, at present, no universally accepted set of ADP security principles.

(7) There is an absence of techniques/methods/models for translating security requirements into technical specifications and their accompanying acceptance criteria.

(8) The development of an ADP certification program without the operational definitions, computer security principles, or techniques/methods/models noted above appears impractical and unrealistic. The certification criteria and standards necessary for a proper evaluation are based upon such fundamentals. This aspect of DCID 1/16 will be difficult to implement.

(9) The difficulty recurs with local "retrofits" or "patches" to current systems. Without criteria and standards, how can we be certain that corrective actions taken result in a truly secure system?

(10) The practical requirements for multilevel secure processing are well known and are multiplying. Present state-of-the-art hardware and software security features, however, are highly vulnerable to subversive penetration attempts. Thus, current capabilities to protect are inconsistent with present/projected needs.

(11) Individual Data Processing Installation/ADP managers need, but do not have, access to a single, comprehensive document which covers all - or even most - aspects of ADP security. Such a directive does not currently exist, notwithstanding DCID 1/16, DCID 6/3 and others.

(12) The existence of a large number of misinformed "experts" and inaccurate or outdated information concerning ADP security procedures have frequently led to overprotective, unnecessarily restrictive and costly regulations and procedures. Conversely, a considerable number of serious security threats exist. These are due to an unawareness of the vulnerabilities and weaknesses in the hardware/software systems used, or inadequate security procedures.

(13) There are a number of other problems (see ESD study), but these appear to be the most difficult and demanding set and should be addressed first.

e. Assumptions: The following assumptions are reflected throughout the plan and form the basis for certain courses of action suggested or implied. The basic assumption underlying the plan is that we can and will solve our ADP security problems. The other assumptions are:

(1) Sooner or later serious penetration attempts against U.S. Government DPIs/ADPS will be made by foreign agents or their accomplices. These attempts will not be limited to military sites.

(2) Those DPIs/ADPS which process large amounts of highly sensitive military, R&D, intelligence & economic info will be the prime targets.

(3) Malicious users pose the greatest risk to contemporary ADPS security.

(4) The actual cost/requirements to penetrate current ADPS is trivial compared to the military and economic value of the information which could be compromised.

(5) Most, if not all, presently installed/planned-for-installation ADPS can be readily penetrated by appropriately trained personnel.

(6) Improvements in any one aspect of ADP security (e.g., procedures, R&D, physical/personnel screening, etc.) will not correct present deficiencies nor satisfy future requirements. A comprehensive approach involving improvements to all aspects is required.

(7) More and increasingly complex multilevel security teleprocessing networks will be established in the near future. They will offer a greater potential for penetration and compromise.

(8) The concern over and the considerable discussion about "ADP security/privacy" reflects the "spirit of the times"; thus, the present environment is considered receptive to solutions to the problems, budgetary considerations notwithstanding.

(9) The increasingly stringent budget restraints under which the Intelligence Community and others are required to operate demand the most realistic and economic approach possible in the use of ADP resources.

(10) RDT&E efforts require practical-minded and centralized guidance if they are to effectively and economically provide the realistic and timely answers needed.

(11) Hardware/software manufacturers and vendors must be convinced that ADP security features will be an integral and indispensable requirement for successful competition in the future.

(12) Practical quantitative and/or operational criteria and standards can be developed for each level of security classification used in the Intelligence Community ADP program.

(13) Significantly greater effectiveness and economy of operation will be achieved through the development and promulgation of such criteria and standards specifically designed to provide the level of protection required vs desired.

(14) Checklists and techniques designed to implement the most reasonable and economical procedures, consistent with an adequate level of protection required, can be developed.

(15) Philosophically, there is no such thing as "absolute security." Absolute security requires infinite time and space. We, and ADPS, however, do not exist in such an abstract concept, but rather in finite time and space. As long as an ADPS is in existence, there can be no "absolute security," either hypothetically or realistically. Ignoring the fact that an ADPS may be "secure" at any one point in time, there is still the possibility that, given sufficient time, resources, etc., it can be compromised. We are still limited to some practical standard(s), which, in turn, is relative to some point(s) on a continuum called "adequate protection". Our objective should be to define such a continuum and identify the appropriate points upon it which satisfy our security requirements.

(16) There are a number of other assumptions to the successful implementation of the plan. For example, competent and technically sophisticated management--this, and others like it, are inherent (assumptions). All others of a critical nature have hopefully been noted.

f. Principal Tasks of the Overall Plan: The items below are listed in relative order of importance or chronological/logical dependence. Taken as a whole, these tasks represent "the plan."

(1) To implement DCID 1/16 and give substance to this plan and any forthcoming regulation/instructions on the subject, an Office of Primary Responsibility (OPR) must be formally designated. An OPR for all aspects of ADP security does not currently exist. Offices of Corollary Responsibility (OCR) must also be identified.

(2) For practical purposes, explicit statements on the specific interrelationships of OPR to OCRs and other Intelligence Community elements must be secured. Each organization must know "who does what to/for whom" if a satisfactory long-term solution is to be found. This is probably the most difficult and important aspect of implementing DCID 1/16.

(3) A DCID or similar publication on the subject of ADP security policy and responsibilities must be developed, coordinated, and promulgated throughout the Intelligence Community. This publication(s) should:

(a) Provide coherent and comprehensive statements on all major aspects of ADP security policy.

(b) Spell out specific responsibilities.

(c) Identify to whom they should be assigned.

The DCID should require Intelligence Community components, to designate an ADPS Security Manager who will be responsible for implementing and managing ADP security policy within that organization and providing for the on-site analysis, testing, and evaluation of the security features of ADPS under their cognizance. Implementing instructions to achieve this objective should be developed as required.

(4) A requirements study should be conducted to more precisely determine what is needed to satisfy the long- and short-range ADP security needs Intelligence Community wide. The study's findings could then be used to "size the problem" more accurately. This should permit better estimates of the probable manpower and other resources required for proper and continuing support in this field, and would essentially lead to a comprehensive "master plan." The security requirements identified in DCID 1/16 as well as an awareness of their ramifications, should provide basic guidance and direction to the study effort.

(5) The development of a practical R&D program designed to investigate and solve ADP security problems is also important. Such R&D efforts should be based upon a realistic R&D master plan which addresses the interrelated fields of intelligence, COMSEC, and EMSEC. Such a plan (and thence program) should provide centralized guidance, control, and an overall perspective for ADP security research and development. Specific R&D projects need to be embedded within the broader context of Intelligence Community needs.

(6) It is necessary to develop an Intelligence Community DCID(s) to provide a comprehensive set of procedures which individual data processing installation managers can use to protect classified information to the level required and in the most economical manner possible. This manual(s) should detail the ADP security threat posed by sophisticated potential enemies and explain in greater detail the practical aspects of new security requirements imposed. It should describe specific procedures and give extensive information on appropriate ADP security techniques. It is perhaps desirable to prepare a number of interrelated, yet different, documents designed to satisfy each level of management/operational control. These could go from more broadly based policy directives down to specific operating instructions for computer operators and customer engineers.

(7) The following task is composed of three interrelated activities which involve:

(a) The creation of ADP security/certification standards, definitions, and inspection/evaluation criteria;

(b) The development of an ADPS certification program; and

(c) The inauguration of an ADPS security inspection activity.

Taken together, they should satisfy the testing, certification, and evaluation requirements imposed by DCID 1/16.

(8) A number of subtasks evolve from the above. For example, an operational definition must be developed for the term "adequate protection". The definition must be further refined and applied in context to each level of security classification (i.e., "adequate protection" for confidential material would most likely be inadequate for top secret material). Such definitions will require the

development of quantitative standards for each classification level as well. The objective is to provide an operational definition which can be expressed in quantitative terms and which will specify "what type" and "how much" protection is necessary for each level of classified material. Normally, the greater the protection provided, the greater the cost.

(9) A series of ADPS security checklists must also be developed. They should be designed to aid the DPI manager, his subordinates, and the ADP security inspector. These checklists should cover all facets of ADPS security, including physical environment, communications, emanations, personnel, and administration.

(10) Wherever technically and economically feasible, standardized security procedures should be developed for each basic series of hardware and software operating systems used for classified processing. The development of such standardized procedures would be priority-ordered relative to Air Force needs by the OPR, according to the:

(a) Importance, volume, and level of classified material processed:

(b) Number and cost of total systems installed throughout the Intelligence Community; and

(c) Level of hardware, software, et al "protection" already provided.

(11) For each system developed, an overall standard and severe series of repeatable tests must be created and used to verify its adequacy to protect each level of classified material. This latter requirement obviously depends upon the creation of quantifiable and operational standards.

(12) A program of continuing education designed to update and correctly inform ADP Managers, as well as individual DPI managers, should be instituted. A critical attitude should be instilled on their part to provide adequate protection, but not "absolute security," Continual questioning of ADP security procedures which appear arbitrary or overly/unnecessarily restrictive should be encouraged, and suggestions for improvement stimulated.

(13) As a first step, the security deficiencies in key ADPS should be identified, characterized, and catalogued. Techniques for appropriate corrective actions should then be identified to the greatest extent possible.

(14) The cost and time required to correct (redesign-repair-reimplement) one or more key ADPS/operating systems to a "secure" system(s) should be determined.

(15) For certain key ADPS, it should be determined if it is more cost-effective for the original designers/developers of the operating system (OS) to redesign-repair-reimplement their own systems than it is for others (e.g., software houses, Government, or captive R&D organizations) to do the job.

(16) It should be determined if it would be more cost-effective for industry, Government, or a joint team to develop a new secure ADPS prototype designed specifically for multilevel (open-use) processing.

(17) The specific requirements for and the advantages and short-comings of an ADP security certification program should be established, at least, before scarce resources are committed by the Intelligence Community.

(18) In conjunction with the foregoing tasks, action could be started to provide the Intelligence Community Managers temporary resources (personnel and equipment) which could assist in implementing improvements to existing ADPS and in establishing whether their ADP security system is providing the level of protection required.

g. Discussion:

(1) The above list of tasks is not meant to be all-inclusive. There are other actions to take and decisions to make. The more important ones are identified here. In any case, it is desirable for the Intelligence Community to be actively concerned with the security of ADPS.

(2) It is academic to accurately estimate resource requirements until an OPR has been designated and until:

(a) A coordinated list of OCR responsibilities have been received and integrated;


- (b) A requirements study can be made; and
- (c) A course of action firmly decided upon.

The same is true regarding the time and logical relationships of one task to the others. These things would naturally follow, once the above items are completed. A separate resource/manning document will be produced and circulated for your review and comments as quickly as possible.

(3) While one may question the \$28 million R&D budget presented in references (ESD Study) it should be apparent that the problems which we must resolve will take considerable time and money. The objectives of adequate protection and the necessity for economic realism require mutual satisfaction.

(4) This draft plan has not been coordinated with nor seen by personnel within the Air Force. It requires your review and suggestions. It does, however, represent a significant amount of previous effort and thought, and is optimistically considered feasible.

(5) A great deal must be done and only limited resources are available to accomplish the tasks noted. While there are many complex problems and few easy or apparent solutions, positive action by the Computer Security Subcommittee should be taken. CSS appears to be the most logical OPR. If the necessary resources can be obtained, the problems can be resolved. The level of effort to be applied by the OPR will undoubtedly depend upon the additional resources it is supplied. If none are provided, little can be done.


FREDERICK R. TUCKER
Air Force Member
Computer Security Subcommittee

Page Denied

Next 2 Page(s) In Document Denied